signature, but instead, the position information itself may be written directly on the disk. In that case also, the invention is effective in preventing pirated disks from being made by copying the marking and its position information.

The optical disk of the invention has a structure such that a reflective film is sandwiched directly or indirectly between two members resistant to laser light and a marking is formed by laser on the reflective film. The above embodiment has described examples in which this structure is used for a piracy prevention technique, but it will be appreciated that such a structure may also be applied to other techniques. In the above embodiment, the optical disk of the invention has been described as being fabricated by laminating two substrates with an adhesive layer interposed therebetween. However, the adhesive layer may be omitted, or instead, a member made of a different material, such as a protective layer, may be used; that is, any suitable structure may be used as long as the reflective film is sandwiched directly or indirectly between two members resistant to laser light. Furthermore, in the above embodiment, the optical disk of the invention has been described as comprising substrates as the members that are laminated together, but other members such as protective layers may be used; that is, any member that has resistance to laser light may be used.

In the above embodiment, a combination of two kinds of cipher, secret key cipher and public key cipher, has been described as a representative example of a combination of multiple kinds of ciphers of different generations, but the invention is not limited to this particular example. For example, as an alternative combination of different generations, public key cipher having a 256-bit secret key, which is less secure but can be processed by a slow CPU, and public key cipher having a 1024-bit secret key, which provides great security but can only be processed by a high-speed CPU, may be used. In this way, with a combination of public key ciphers having different security levels, the same effect of preserving compatibility between different generations can be obtained. Furthermore, a combination of three kinds of ciphers of different generations, such as secret key cipher, low-security public key cipher, and high-security public key cipher, may also be used.

What is claimed is:

1. A marking forming apparatus comprising:

marking forming means for applying at least one marking to at least one reflective film formed to a disk;

marking position detecting means for detecting at least one position of said marking; and

position information output means for outputting said detected position as position information of said marking.

2. A marking forming apparatus according to claim 1, further comprising position information writing means for writing at least said output position information or information concerning said position information to said disk or to a different medium.

3. A marking forming means according to claim 2, wherein said position information writing means includes encrypting means for encrypting at least said output position information or information concerning said position information, and writes contents thus encrypted to said disk.

4. A marking forming apparatus according to claim 3, wherein when the encrypting means performs the encryption, it uses a secret key of a public key encryption function.

5. A marking forming apparatus according to claim 3, wherein said encrypting means includes

first encrypting means for encrypting software feature information concerning features of software contents written to said disk and a sub public key of a public key encryption function by using a master secret key of said public key encryption function, and

second encrypting means for encrypting said position information or information concerning said position information by using a sub secret key corresponding to said sub public key,

and the writing at least said output position information or information concerning said position information means writing contents encrypted by said first encrypting means and contents encrypted by said second encrypting means to said disk.

6. A marking forming apparatus according to claim 2, wherein said position information writing means includes digital signature means for applying a digital signature to at least said output position information or information concerning said position information,

and the writing at least said output position information or information concerning said position information means writing information concerning a result of said digital signature application to said disk.

7. A marking forming apparatus according to claim 6, wherein when said digital signature means applies said digital signature, it uses a secret key of a public key encryption function.

8. A marking forming apparatus according to claim 6, wherein

said digital signature means includes

first digital signature means for applying a digital signature to software feature information concerning features of software contents written to said disk and to a sub public key of a public key encryption function by using a master secret key of said public key encryption function, and

second digital signature means for applying a digital signature to said position information or information concerning said position information by using a sub secret key corresponding to said sub public key,

and the writing at least said output position information or information concerning said position information means writing a result of the application of said digital signature by said first digital signature means and a result of the application of said digital signature by said second digital signature means to said disk.

9. A marking forming apparatus according to claim 2, wherein the position information writing means writes coexistently such informations that are processed by using plural kinds of encryption techniques or digital signature techniques with regard to a same position information.

10. A marking forming apparatus according to claim 4, 5, 7, or 8, wherein said public key encryption function is an RSA function or an elliptic function.

11. A marking forming apparatus according to claim 10, wherein said disk is constructed by laminating two disks together.

12. A method of forming a laser marking to an optical disk, comprising the steps of:

forming at least one disk;

forming a reflective film to said formed disk;

laminating two disks together, said disks including at least one disk with said reflective film formed thereon; and

forming at least one marking by a laser on said reflective layer of the laminated disks.

13. A reproduction apparatus comprising:

position information reading means for reading position information of at least one marking or information

concerning said position information, said marking being formed to at least one reflective film formed to a disk and being detected for a position thereof, at least the position thus detected being output as said position information of said marking;

marking reading means for reading information concerning at least one actual position of said marking;

comparing/judging means for performing comparison and judgement by using a result of reading by said position information reading means and a result of reading by said marking reading means; and

reproducing means for reproducing recorded data on said optical disk in accordance with a result of the comparison and judgement performed by said comparing/judging means.

**14**. A reproduction apparatus according to claim **13**, wherein at least said output position information or information concerning said position information is written to said disk by position information writing means.

**15**. A reproduction apparatus according to claim **14**, wherein

said position information writing means includes encrypting means for encrypting at least said output position information or information concerning said position information, and

said position information reading means includes decrypting means corresponding to said encrypting means, and by using said decrypting means, decrypts said encrypted position information or information concerning said position information.

**16**. A reproduction apparatus according to claim **15**, wherein when the encrypting means performs the encryption, it uses a secret key of a public key encryption function, and

said decrypting means performs the decryption by using a public key corresponding to said secret key.

**17**. A reproduction apparatus according to claim **15**, wherein

said encrypting means includes

first encrypting means for encrypting software feature information concerning features of software contents written to said disk and a sub public key of a public key encryption function by using a master secret key of said public key encryption function, and

second encrypting means for encrypting said position information or information concerning said position information by using a sub secret key corresponding to said sub public key,

and said decrypting means includes

first decrypting means for decrypting said encrypted software feature information and the encrypted sub public key of said public key encryption function, by using a master public key corresponding to said master secret key, and

second decrypting means for decrypting said encrypted position information or information concerning said position information by using the sub public key thus decrypted.

**18**. A reproduction apparatus according to claim **14**, wherein

said position information writing means includes

digital signature means for applying a digital signature to at least said output position information or information concerning said position information, and writes information concerning a result of said digital signature application to said disk,

and said position information reading means includes

authenticating means corresponding to said digital signature means, and

position information extracting means for obtaining said position information from an authentication process performed by said authenticating means and/or from said information concerning the result of said digital signature application,

when an output indicating correctness of said authentication result is produced from said authenticating means, said comparing/judging means performs the comparison and judgement by using the position information obtained by said position information extracting means and the result of reading by said marking reading means, and when said output indicating correctness is not produced, the reproduction is not performed.

**19**. A reproduction apparatus according to claim **18**, wherein

when said digital signature means applies said digital signature, it uses a secret key of a public key encryption function, and

said authenticating means performs said authentication by using a public key corresponding to said secret key.

**20**. A reproduction apparatus according to claim **18**, wherein

said digital signature means includes

first digital signature means for applying a digital signature to software feature information concerning features of software contents written to said disk and to a sub public key of a public key encryption function by using a master secret key of said public key encryption function, and

second digital signature means for applying a digital signature to said position information or information concerning said position information by using a sub secret key corresponding to said sub public key,

and the writing at least said output position information or information concerning said position information means writing a result of the application of said digital signature by said first digital signature means and a result of the application of said digital signature by said second digital signature means to said disk,

wherein said position information reading means includes:

authenticating means for authenticating said digital signature-applied software feature information and sub public key of said public key encryption function, by using a master public key corresponding to said master secret key, and

position information extracting means for obtaining said position information from said authentication process thereof and/or from the result of said digital signature application by using the sub public key obtained from said authentication process and/or from the result of said digital signature application,

and when an output indicating correctness of said authentication result is produced from said authenticating means, said comparing/judging means performs the comparison and judgement by using the position information obtained by said position information extracting means and the result of reading by said marking reading means, and when said output indicating correctness is not produced, the reproduction is not performed.

**21**. A reproduction apparatus according to any one of claims **13** to **20**, wherein the reproduction is not performed

when, as a result of said comparison and judgement, the result of reading by said position information reading means and the result of reading by said marking reading means do not agree with each other.

**22.** A reproduction apparatus according to claim **16**, **17**, **19**, or **20**, wherein said public key encryption function is an RSA function or an elliptic function.

**23.** A method of manufacturing an optical disk, comprising the steps of:

forming at least one disk;

forming a reflective film to said formed disk;

applying at least one marking to said reflective film;

detecting at least one position of said marking; and

outputting said detected position as position information of said marking, and encrypting said information for writing to said disk.

**24.** A method of manufacturing an optical disk, comprising the steps of:

forming at least one disk;

forming a reflective film to said formed disk;

applying at least one marking to said reflective film.

detecting at least one position of said marking; and

outputting said detected position as position information of said marking, and applying a digital signature in relation to said position information for writing to said disk.

**25.** An optical disk wherein at least one marking is formed by a laser to at least one reflective film of the disk holding data written thereon and at least position information of said marking or information concerning said position information is written to said disk in an encrypted form or with a digital signature applied thereto.

**26.** An optical disk having a structure such that at least one reflective film is one of sandwiched directly and sandwiched indirectly between two members formed from material resistant to laser light,

wherein at least one marking is formed by a laser to said reflective film.

**27.** A marking forming apparatus according to claim **9**, wherein said disk is constructed by laminating two disks together.]

* * * * *